

Stimulus Bill Dramatically Modifies HIPPA Privacy & Security

New Guidance

- American Recoveries and Reinvestment Act of 2009 (“ARRA”) modifies HIPPA rules
- Applying Security rules to business associates (BAs)
- New breach notification rules
- New Privacy Rules - some may apply to business associates
- Increased penalties
- By August 2009 HHS will designate an individual in each regional office to offer guidance and education to covered entities.
- By February 2010 HHS will conduct education initiatives to educate individuals about uses of PHI

Applying Security Rules to Business Associates

- Business associates were “indirectly” covered before, through business associate agreement with covered entity.
- BA contract followed many HIPPA rules but not all
- ARRA now directly applies most HIPPA Security Rules (and some Privacy Rules) directly to BA
- Security Rules that now apply directly to business associates:
 - 45 CFR 164.308: Administrative Safeguards
 - 45 CFR 164.310: Physical Safeguards
 - 45 CFR 164.312: Technical Safeguards
 - 45 CFR 164.316: Policies, Procedures, and Documentation
- Additional requirements of ARRA that related to security and are made applicable to covered entities: (1) apply to BA; and (2) must be incorporated into BA agreement between BA and covered entity (including civil and criminal penalties)

New Breach Notification Rules

- If: (1) covered entity accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses “unsecured protected health information” and (2) there is a “breach” of such information; and (3) the breach is “discovered” by covered entity; then (4) notification rules apply
- Covered entities and, apparently, business associates follow rule
- “Accesses, maintains...unsecured PHI”;
- “Unsecured PHI”-PHI not secured through technology or methodology approved by HHS
- “Breach” is: (1) unauthorized (2) acquisition, access, use or disclosure of PHI which (3) compromises security or privacy of PHI (4) except where unauthorized person would not reasonably have been able to “retain” PHI

Breach Does Not Include

- (1) unintentional (2) acquisition, accesses, use or disclosure of PHI by (3) an employee or agent of covered entity or business associate if (4) made in good faith and (5) within course and scope of employment or other relationship if (6) information not further acquired, access, used or disclosed by any person

- (1) Inadvertent (2) disclosure (3) from an individual who is authorized to access PHI (4) at a facility operated by a covered entity or BA to (5) another similarly situated individual (6) at the same facility and (7) any such PHI received as a result of disclosure is (8) not further acquired, accessed, used or disclosed without authorization by any person.

What Happens If Breach Occurs

- Make notification without “unreasonable delay”, no later than 60 calendar days of breach discovery
- Burden of proof on covered entity/ BA to show timeliness, including evidence demonstrating necessity of delay
- Notice must be provided to individual
- Written notice by first-class mail to individual (or next of kin) at last known address or, if specified by an individual, email

Breach Rules - Time and Method of Notice

- Notice must be provided to prominent media outlets in state or “jurisdiction” is or reasonably believed to have been, accessed, acquired or disclosed during breach
- If breach of 500+ individuals, provide notice to HHS “immediately”
- If breach is less than 500 individuals, maintain log of breach and annually submit to HHS
- Breach notifications may be delayed for national security or law enforcement reasons

Breach Rules - Include in Content of Notification

- Brief description of what happened, including date of breach and date discovered
- Types of unsecured PHI involved (e.g., name, Social Security number, date of birth, home address, account number)
- Steps individual should take to protect from potential harm
- What covered entity is doing to investigate the breach, mitigate losses and protect against further breaches
- Contact procedures for individuals to ask questions; shall include toll-free phone number, email address, web site or postal address
- HHS to issue interim final regulations by August 16, 2009.
- Regulations apply to breaches 30 days after date of publication

Applying Privacy Rules to Business Associates

- If BA receives PHI pursuant to BA agreement, it can use and disclose PHI only if use or disclosure complies with “each applicable requirement of section [45 CFR] 164.504(e)”
- 164.504(e) typical BA provisions-and include references to many other sections of HIPPA (e.g., 164.524 for making PHI available; 164.526 for amending PHI, etc.)
- Currently, covered entity must terminate BA agreement with BA or report to HHS a BA’s uncured breach of BA agreement
- Now, rule applies the same way for BAs (terminate BA agreement or report covered entity’s breach to HHS, if covered entity fails to cure breach)
- Effective date Feb. 17, 2010

New Restriction Request Rules

- Currently, individual can make restriction request under 164.522 – and covered entity usually need not follow it
- Under ARRA, covered entity must comply with request if disclosure is to a health plan for purposes of carrying out payment or health care operations (but not treatment) and PHI pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full

New Guidance on “Minimum Necessary”

- Currently, disclosure of PHI must be “minimum necessary” amount
- Under ARRA “minimum necessary” means “limited data set” info
- HHS to issue guidance on meaning of term by August 2010

New Accounting Rules for Electronic Health Records (EHRs)

- “EHR” is electronic record of health-related info on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff
- Currently, disclosure accounting rules requires covered entity to track all disclosures of PHI but contains big exception for treatment, payment or health care operations
- Under ARRA, if covered entity uses or maintains EHRs with respect to PHI, individual has right to accounting of such disclosures made by covered entity during three year prior to date on which accounting is requested
- HHS to issues regulations by August 2009
- In responding to accounting request, covered entity can provide full accounting (i.e., gather all data from all BAs, aggregate together) or refer individual to BAs (give list of BAs)
- Effective date for EHR acquired by covered entity prior to January 1, 2009, only for disclosures made on and after January 1, 2014
- If acquire EHR after January 1, 2009, rule applies as of later(1)January 1,2011; or (2) date EHR acquired

Prohibiting Sale of EHRs or PHI

- Covered entity and BA cannot “directly or indirectly receive remuneration” in exchange for any PHI unless covered entity obtained valid authorization from individual (and authorization must specify that remuneration is acceptable)
- Exceptions (e.g., can receive a few dollars from individual for copying medical records; research, treatment)
- Effective date is 6 months after final regulations

Right to Access and EHRs

- Currently, individual can access PHI held in “designated record set”
- Under ARRA, if covered entity has EHR:
- Individual has right to obtain copy of info in an electronic format and, if individual chooses, to direct covered entity to transmit copy directly to an entity or person designated by the individual (choice must be “clear, conspicuous, and specific”)

- Effective date is February 2012

Increased Penalties and Enforcement

- Penalties must be imposed if HIPPA violation due to “willful neglect” (and HHS required to investigate)
- Funds from imposed penalties are transferred to Office for Civil Rights (part of HHS) to be used for enforcing HIPPA
- By August 2010 HHS proposal on how individuals harmed can recover a percentage of any civil monetary penalty to settlement
- State attorney generals can sue to enforce and seek attorney fees
- HHS audits are now required
- Currently, general penalty is \$100 per HIPPA violation (cap of \$25,000 for multiple violations in same year)
- Under ARRA, same \$100 if did not know of violation and would not have known even with reasonable diligence
- Now \$1,000 penalty if due to reasonable cause and not willful neglect (\$100K cap)
- Now \$10,000 - \$ 50,000 penalty if willful neglect (\$250K -\$1.5M cap)

Other Important Changes

- “Vendors” of “personal health records” (i.e., electronic records managed, shared and controlled by or primarily for individual) subject to new breach and security rules
- Organization providing data transmission of PHI needs BA agreement